

What are the permissions needed for Microsoft Graph?

Last Modified on 05/03/2024 4:52 pm EDT

Permissions for Microsoft Graph

The permissions needed vary depending on whether or not you enable SSO and how you want List Expansion to be handled (Client-Side, Server-Side, or both). Each possible configuration is outlined below. You can skip to the PoliteMail default configuration, Server-Side Expansion, by clicking [here](#).

OAuth (SSO) login to PoliteMail

Small lists (< 1000 members) can be expanded via MAPI in Outlook Desktop.

List Handling		
List Expansion Methods Enabled		
	Client	Server
EWS	<input type="checkbox"/>	<input type="checkbox"/>
Graph	<input type="checkbox"/>	<input type="checkbox"/>
MAPI	<input type="checkbox"/>	

Graph Permission	Application or Delegated
User.Read	Delegated
offline_access	Delegated
openid	Delegated
profile	Delegated

Client-Side Expansion of Entra ID Groups

Client (delegated) expansion is not currently supported from PoliteMail Online or PoliteMail for Microsoft 365.

List Handling		
List Expansion Methods Enabled		
	Client	Server
EWS	<input type="checkbox"/>	<input type="checkbox"/>
Graph	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MAPI	<input type="checkbox"/>	

Graph Permission	Application or Delegated
offline_access	Delegated
openid	Delegated
profile	Delegated

User.Read	Delegated
GroupMember.Read.All	Delegated
MailboxSettings.Read	Delegated
OrgContact.Read.All	Delegated
People.Read.All	Delegated
User.Read.All	Delegated

Client-side expansion of Entra ID Groups and Dynamic Distribution Groups (Exchange) via EWS

List Handling

List Expansion Methods Enabled

	Client	Server
EWS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Graph	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MAPI	<input type="checkbox"/>	<input type="checkbox"/>

Graph Permission	Application or Delegated
offline_access	Delegated
openid	Delegated
profile	Delegated
User.Read	Delegated
GroupMember.Read.All	Delegated
MailboxSettings.Read	Delegated
OrgContact.Read.All	Delegated
People.Read.All	Delegated
User.Read.All	Delegated
EWS.AccessAsUser.All	Delegated

Server-Side Expansion of Entra ID Groups

This is the default PoliteMail SaaS configuration requirement for M365 integration, and the most often requested.

List Handling

List Expansion Methods Enabled

	Client	Server
EWS	<input type="checkbox"/>	<input type="checkbox"/>
Graph	<input type="checkbox"/>	<input checked="" type="checkbox"/>
MAPI	<input type="checkbox"/>	<input type="checkbox"/>

Graph Permission	Application or Delegated
offline_access	Delegated

openid	Delegated
profile	Delegated
User.Read	Delegated
GroupMember.Read.All	Application
MailboxSettings.Read	Application
OrgContact.Read.All	Application
People.Read.All	Application
User.Read.All	Application

There is no scenario where PoliteMail needs access to all mailboxes; to restrict read.all and limit permissions to a specific mailbox, e.g. a service account, implement an Application Access Policy (Application Scopes) as described in this Microsoft article.

Server-side expansion of Entra ID Groups and Dynamic Distribution Groups (Exchange) via EWS

List Handling

List Expansion Methods Enabled

	Client	Server
EWS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Graph	<input type="checkbox"/>	<input checked="" type="checkbox"/>
MAPI	<input type="checkbox"/>	<input type="checkbox"/>

Graph Permission	Application or Delegated
offline_access	Delegated
openid	Delegated
profile	Delegated
User.Read	Delegated
GroupMember.Read.All	Application
MailboxSettings.Read	Application
OrgContact.Read.All	Application
People.Read.All	Application
User.Read.All	Application
full_access_as_app (Single Mailbox Application Scope)	Application

All Features Enabled

List Handling

List Expansion Methods Enabled

	Client	Server
EWS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Graph	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MAPI	<input type="checkbox"/>	<input type="checkbox"/>

Graph Permission	Application or Delegated
offline_access	Delegated
openid	Delegated
profile	Delegated
User.Read	Delegated
GroupMember.Read.All	Both
MailboxSettings.Read	Both
OrgContact.Read.All	Both
People.Read.All	Both
User.Read.All	Both
full_access_as_app (Single Mailbox Application Scope)	Application
EWS.AccessAsUser.All	Delegated